July 2007

Federation News

Volume I, Issue 2

New Relying Parties:

- Department of Defense's *MyPay*
- Department of Labor's *OSHA Webservices*
- General Services Administration's *E-Travel*
- Department of State's *Webmove*

eRulemaking Implements E-Authentication Ahead of Schedule

When the Environmental Protection Agency eRulemaking Initiative Program Management Office (PMO) kicked off the E-Authentication project last September, they had barely 90 days to meet the mandated December 31, 2006 deadline to credential the first Federal Docket Management System (FDMS.gov) user. With the holiday season approaching, the eRulemaking program staff – with fewer than ten people – had their hands full deploying FDMS.gov to multiple federal agencies, managing a new version release, and planning a number of public outreach events. To meet the mandated deadline, the PMO and its systems integration partner, Lockheed Martin, formed a task team and put a plan in place to put the project on a fast track for completion by mid-December.

The plan worked. The first FDMS.gov user was credentialed on FDMS.gov on December 20, 2006 – 11 days ahead of schedule. FDMS includes the system architecture and web-based functionality that enables federal agency users to access a secure system via FDMS.gov to facilitate searches, manage public comments on federal regulations, and make information available to the public on Regulations.gov. "eRulemaking's three-month deployment was the fastest deployment of a viable E-Authentication solution to date," said Georgia Marsh, Acting Program Executive, E-Authentication Solution,

(Continued on page 6)

Regulations.gov facilitates public participation in the federal regulatory process by improving the public's ability to find, view, and comment on federal regulatory actions.

New Architecture Approved: SAML 2.0 is Ready for Business

The E-Authentication PMO has revised its architecture to incorporate the Security Assertion Markup Language (SAML) 2.0 specification from OASIS to better meet the authentication needs of agencies. The revised architecture incorporates an additional adopted scheme and interface specification letting agencies take advantage of the enhanced functionality included in OASIS' new SAML specification.

The process to revise the architecture was rigorous. The E-Authentication PMO conducted an interoperability event in the Interoperability Lab to determine the capability of various vendors to comply with the SAML 2.0 specification. The E-Authentication PMO also talked with agencies to identify which features were necessary, as well as other features that would be most valuable to them. Working on

(Continued on page 6)

The SAML 2.0 specification from OASIS provides agencies with more functionality to support their electronic authentication needs.
http://www.oasis-open.org

Federation News

Manager's Corner

PRINCIPLE

The E-Authentication PMO is customer-focused.

The E-Authentication PMO meets the authentication needs of its customers and delivers value to them in doing so.

On June 6, 2007, the E-Authentication Executive Steering Committee formally endorsed a new business model approach to provide agencies with policy-compliant electronic authentication services under a fee-for-service model. This was a major milestone and a turning point in the history of E-Authentication – it marked the beginning of the transition from a "mandate-driven" initiative to a "market-driven" business line.

Incorporating input from agencies and industry, the new business model delivers value to our agency customers and provides them with the choice and flexibility to meet their electronic authentication needs. Already, there have been a number of very positive conversations with agencies who are interested in using our services (Federation membership, credential services, and integration and technical support services), and the PMO will be following up with all our agency customers over the course of the summer to customize a package of services for each of them. Over the summer the PMO will establish new contract vehicles and continue certifying more products as interoperable to make sure services are fully available by the end of 2007 – the PMO will be "open for business" as planned.

Your comments on our new service offering are welcome and we look forward to meeting with each agency during the next few months to discuss how the PMO can deliver the best E-Authentication services to meet your agency's needs. Please contact me at georgiak.marsh@gsa.gov or (703) 872-8614 if you would like to get more information or set up a meeting to begin discussions on how E-Authentication can help you or your agency.

Georgia K. Marsh
Acting Program Executive,
E-Authentication

E-Authentication Service Offering

Federation Membership

Agency participation in the U.S. E-Authentication Identity Federation.

Credential Services

Identity proofing, credential issuance, credential life-cycle management services, and value-added authentication services agencies need to authenticate users of their applications.

The Managed Validation and Translation Service (MVTS) enables PKI certificates (such as those issued under HSPD-12) to be validated and used for access to assertion-based applications.

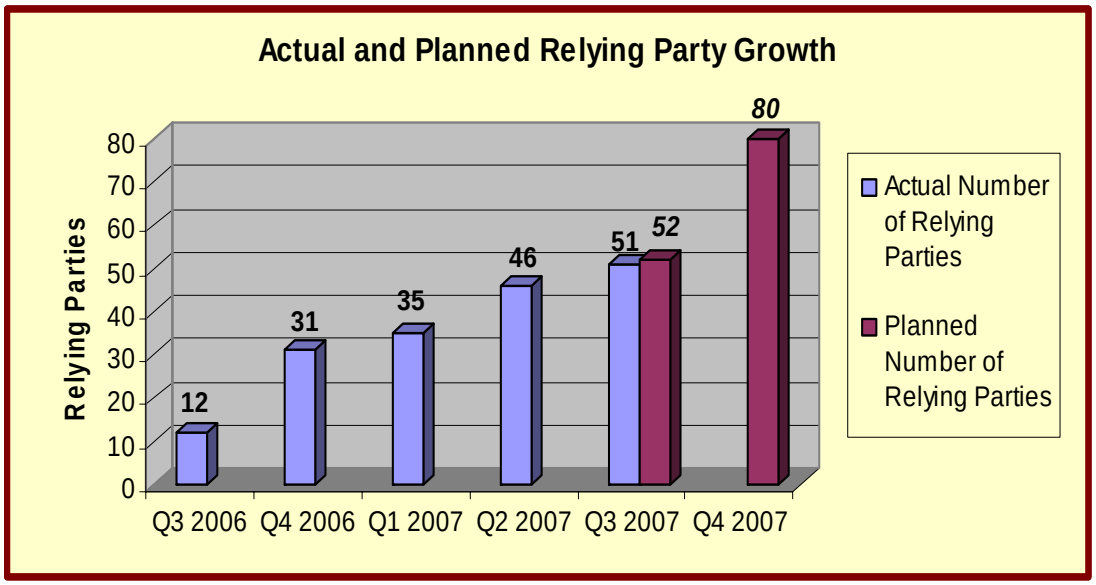
Integration and Technical Support Services

Basic – Technical baseline planning, support for product selection, setup of test environment, acceptance testing, node connection testing, on-boarding services, and deploy E-Authentication.

Preferred – Technical baseline planning, support for product selection, setup of test environment, vendor testing MVTS, on-boarding services and deploy E-Authentication.

Premium – All of the Basic and Preferred services plus services such as support to develop a detailed project plan; assess risks; select a technical approach; select approved products, integration services, and credential service providers; and deploy E-Authentication.

The U.S. E-Authentication Identity Federation Continues to Grow



Federation membership continues to grow with the number of applications anticipated to more than double during FY 2007. The E-Authentication PMO is on pace to hit its FY 2007 target of 80 Relying Parties within the Federation.

Schedule of Events

- July 19 (2-4 PM @ PMO) Vendor Council Meeting
- July 28 (1-3 PM @ PMO) Technical Work Group Meeting
- August 14 (9-4 PM @ PMO) Vendor Day
- August 16 (1-3 PM @ PMO) Federation User Group Meeting
- August 30 (1-3 PM @ PMO) Technical Work Group Meeting
- September 12 (2-4 PM @ GSA HQ) Executive Steering Committee Meeting
- September 19 (9-11 AM @ PMO) Relying Party Member Council Meeting
- September 20 (9-11 AM @ PMO) CSP Member Council Meeting
- September 27 (1-3 PM @ PMO) Technical Work Group Meeting

GSA ITS 2007 Network Services Conferences
August 6-9, Adams Mark Hotel, Denver, CO
http://www.gsanetworkservices.org
E-Authentication Solutions Training
Wednesday, August 8: 10:30-11:45 AM
Thursday, August 9: 10:30-11:45 AM

Get E-Authentication Help

The E-Authentication Help Desk assists end users and Federation members with issues related to their E-Authentication-enabled applications and credential services.

The E-Authentication Help Desk also maintains Federation member contact information and manages E-Authentication Portal maintenance activities. Please send updated contact information to eauth.service.help@gsa.gov.

If you need to contact the E-Authentication Help Desk, you can use one of the e-mail addresses listed below or call toll-free (877) 307-5528.

User Issues
eauth.portal.help@gsa.gov

Federation Member Issues
eauth.service.help@gsa.gov

Transaction Reports (submit by 10th)
eauth.reports@gsa.gov

Documented Issues
eauth.reports@gsa.gov

The E-Authentication Help Desk is ready to address questions and issues from Federation members and their end users.

E-Authentication Establishes Performance Measures

With the E-Government initiatives maturing and reaching full deployment, attention is increasingly on initiative performance and delivery of results.

What gets measured gets done. In April 2007, the E-Authentication PMO met with its Office of Management and Budget (OMB) Portfolio Manager to agree on the E-Authentication performance measures going forward to increase the focus on performance and the delivery of results. This effort was conducted for all of the E-Government initiatives and the performance information collected from the initiatives will be published quarterly on the OMB E-Gov web site at http://www.whitehouse.gov/omb/egov/c-7-index.html.

E-Authentication Metrics

- % of agencies using E-Authentication [Adoption/Participation]
- % of applications accepting policy-compliant credentials [Adoption/Participation]
- % of applications accepting policy-compliant credentials from E-Authentication [Adoption/Participation]
- # of transactions processed using E-Authentication service [Usage]
- Customer satisfaction [Customer Satisfaction]
- % of applications accepting ONLY policy-compliant credentials [Adoption/Participation]
- Cost avoidance/savings from use of E-Authentication's Authentication Service Component [Cost Savings/Avoidance]

The performance measures are in five key areas of focus:

Adoption/Participation – The degree to which the relevant community (agencies, bureaus, other organizations) participates in the initiative. Participation is demonstrated by contribution of information, involvement in governance, etc.

Usage – The level of use by the targeted end user.

Customer Satisfaction – End user satisfaction with the initiative's products and/or services.

Cost Savings/Avoidance – The degree to which the Initiative results in cost savings, cost avoidance, and reduction in burden from both a government and citizenry perspective.

Efficiency – The degree to which the Initiative results in process improvements such as a decrease in time and/or an increase in productivity.

The performance measures established by the E-Authentication PMO and OMB will provide additional insight into the state of agency adoption and serve to demonstrate the value being delivered to agencies through the use of E-Authentication-approved products and services.

Recognizing the service offering will evolve over time to better meet the needs of agency customers, the E-Authentication Executive Steering Committee is also launching a Metrics Working Group to identify additional performance measures to more effectively assess and better manage the E-Authentication service offering.

If you participate on the E-Authentication Executive Steering Committee and are interested in getting involved with the Metrics Working Group or know someone who is, please contact the E-Authentication PMO at eauthenticationpmo@gsa.gov or (703) 872-8570.

Interfederation: Higher Education and E-Authentication

For those of us who go back a few years, it is striking to see the parallels between the development of the original Internet and the work now happening to build a global network of trust connectivity leveraging the Internet federated identity approaches. In that comparison, one could point to no more important piece of work than the interfederation peering initiative now underway between the U.S E-Authentication Identity Federation and the InCommon Federation. It could pioneer the transition of isolated networks of identity into an Internet-scale trustworthy infrastructure.

InCommon is the identity federation representing the U.S. research and higher education (R&E) community. Growing steadily, it now has over fifty members, representing both academia and important business partners, from scholarly and popular content providers to outsourced service providers. InCommon mirrors developments in the R&E sectors in many other countries, and like many of them, is based on Shibboleth, an open-source fully SAML-compliant software system particularly suited for multi-member full function federations and is compatible with commercial products.

The interests of the InCommon community in interacting with the federal agencies are legion. Researchers want to access agency grant processes, from submission to peer review, using their campus online credentials. Universities want to improve the business processes for students, from facilitating their direct access to student loan and other education-related agency applications to streamlining federal reporting processes. Federal research sites want to enable the use of campus credentials to improve security. The relationships flow both directions; agency professional staff want to use their agency credentials to work with research partner sites on campuses, and vice versa.

Work is actively underway now to develop mechanisms, both technical and policy, to peer between InCommon members and federal agencies participating in the U.S. E-Authentication Identity Federation. The discussions include attributes to be exchanged (including level of assurance), legal structures, financial issues, metadata exchanges, and operational procedures. Little noted, but of great consequence, is the careful way that individual privacy is being protected in this work as well. When the peering work is successful, it will trigger the creation of a full federated trust mechanism with a scope as large as the Internet itself.

Ken Klingenstein
Director, Internet2 Middleware and Security
University of Colorado at Boulder
Boulder, CO

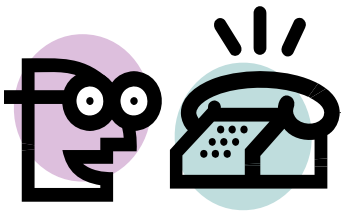
Interfederation Benefits

- Access to a large base of credentialed end users
- Resource sharing and cost saving opportunities
- Policy consistency between the Federal Government and the higher education community
- Better end user experience
- Improved security and privacy

The mission of the InCommon Federation is to create and support a common framework for trustworthy shared management of access to on-line resources in support of education and research in the United States.
http://www.incommonfederation.org

Federation News

A Publication by the U.S. E-Authentication Identity Federation
E-Authentication Program Management Office
Integrated Technology Service
Federal Acquisition Service
U.S. General Services Administration
Crystal Park One
2011 Crystal Drive, Suite 911
Arlington, VA 22202
(703) 872-8570
eauthenticationpmo@gsa.gov
http://www.cio.gov/eauthentication
http://www.gsa.gov/its



We want to hear from you!

(Continued from page 1)

U.S. General Services Administration (GSA).

What were eRulemaking's keys to success?

Prior completion of an E-Authentication proof-of-concept. This provided important and useful information about the scope of work and magnitude of the challenge. *(Patrick Micielli, eRulemaking PMO Contract Officer and Technical Lead)*

Setting realistic, actionable milestones and clearly defined roles. Weekly status calls with the PMO, the GSA E-Authentication staff, and our Oracle representatives helped keep everyone on track. Also, mitigate risk by planning for contingency. We chose the latest Oracle software, which was untested by the GSA E-Authentication Interoperability Team. We mitigated that risk by identifying backup alternatives and securing Oracle services and GSA E-Authentication support. *(Vic Forney, Lockheed Martin eRulemaking Team Operations and Technical Manager)*

Utilizing E-Authentication tools and support. The E-Authentication deployment process helped set expectations for the amount of time and level of effort required for each deployment activity. The E-Authentication Implementation Team also provided support during the test and evaluation phase – in the GSA E-Authentication Lab, we had a controlled environment for conducting testing, and the staff was very accommodating. *(Pete Koumoutseas, Lockheed Martin E-Authentication Project Coordinator)*

The eRulemaking project team offered several "best practice tips" for other programs deploying E-Authentication:

Work collaboratively, anticipate issues, and be flexible. Any technical project can bring unexpected challenges – effective planning can help avoid/mitigate problems or delays.

Understand your organization's procurement process and procurement cycle lead times. The E-Authentication Team provides detailed information on products it supports. Take some time to determine whether you own the products you will need for E-Authentication. What do you have to purchase, and how long will it take to obtain it?

Make the most of the time you have with all of your partners in the project during project status meetings. This is new ground for most people, so structure meetings to allow time for people to ask questions, capture action items, recap discussion points and issues, and discuss next steps.

The eRulemaking FDMS application is available at FDMS.gov and available to the public at Regulations.gov.

(Continued from page 1)

behalf of the agencies, the E-Authentication PMO discussed the Government's prioritized requirements with the vendors so they could include those features in their products, resulting in better product capabilities available to agencies. The vendors then participated in another interoperability event to demonstrate their products' capabilities, their ability to meet the Government's requirements, and their ability to interoperate with other vendors' products.

Agencies, vendors, and other external stakeholders commented extensively on the revised suite of architecture documents. After the comments were incorporated, the new architecture documents were finalized and approved by the Technical Working Group. A tiger team within the Technical Working Group is now addressing the issues associated with migrating agencies and CSPs to the new architecture.